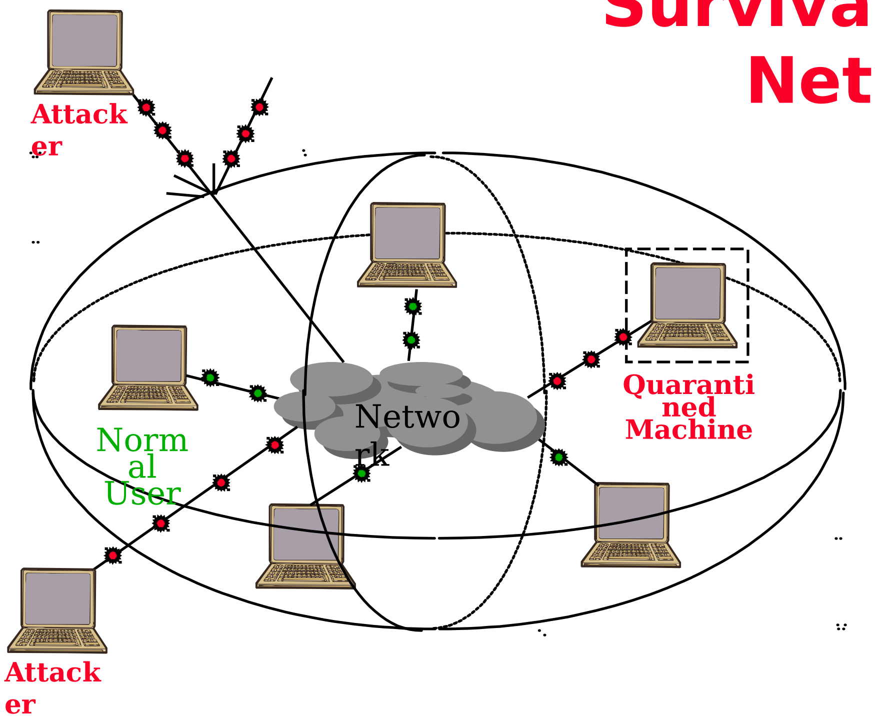
Survivable Active Networks



New Ideas

- high-level language to capture security-related behaviors -- designed for simplicity, clarity, conciseness and detection system robustness
- efficient techniques for checking/enforcing conformity of process or host behavior with specifications
- techniques to prevent compromised programs from damaging system while they continue to run -- enables observation/tracing of attacker
- active-networking based techniques for isolating and locating attacker

Impact

- ***proactive/preventive*** approach will provide better protection for mission-critical systems, e.g., military, telecom, banking/commerce
- ***automated response*** capabilities will enable
  - isolation and containment of damage
  - evidence collection leading to identification of attack source and greater knowledge of exploits
  - cost-effective operation
- ***programmability*** empowers local security officer to create and install

Schedule

Design all techniques

First implementations of detection and isolation techniques

Implementation of coordination and identification techniques

Demo detection and isolation techniques on single host

Integration of all techniques on network of hosts

Demo effectiveness of system by testing against attack scenarios

Aug 97 Start

Aug 98

Aug 99

Aug 00 End

Telcordia: M. E. Segal; Iowa State U.: R. C. Sch